

CUBE および CUCM の設定 音声 セキュリティ 機能

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[関連情報](#)

概要

この資料に Cisco Unified Border Element (CUBE) と Cisco Unified Communications Manager (CUCM) 間のセキュリティを設定する方法を記述されています。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Unified Communications Manager (CUCM)
- Cisco Unified Border Element (CUBE)
- Transport Layer Security (TLS)
- 保護して下さいリアルタイムトランスポートプロトコル (SRTP) を
- Real-Time Transport Protocol (RTP; リアルタイム転送プロトコル)
- Session Initiation Protocol (SIP)
- ユーザ データグラム プロトコル (UDP)
- インターネットテレフォニー サービスプロバイダー (ITSP)

使用するコンポーネント

このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。対象のネットワークが実稼働中である場合には、どのような作業についても、その潜在的な影響について確実に理解しておく必要があります。

背景説明

CUCM で TLS および SRTP に CUBE の RTP の設定方法

この設定の前に、CUCM はセキュリティ イネーブルのミックスマードに調整する必要があります。

CUBE はインターネットワークオペレーティングシステム (IOS) 認証局 (CA) として、CUCM 認証で署名する自己機能します。

ラボ コールフロー

CP-8945 電話 > CUCM- (SIP/TLS) - CUBE > (SIP/UDP) - その他の国々は ITSP (RTP) を > 電話模倣します

SRTP は CP-8945 電話と CUBE の間にあります

CP-8945 電話番号 2088 年は 2088 年の方の ITSP からのコールに、表示コマンドに基づいています。

設定

ステップ 1. クロックを設定するために、clock set コマンドを実行するか、または NTP を設定して下さい。

```
Set clock 8:00:00 01 JAN 2012
```

Or

```
Ntp server x.x.x.x
```

```
ntp source FastEthernet0/0
```

```
clock timezone AEST +10
```

Configure gateway to act as http server: "ip http server"

ステップ 2. 設定 IOS PKI サーバ及び Trustpoints (CA としてローカルルータ)

```
crypto pki server iosca
  database level complete
  database url nvram:
  grant auto
  lifetime certificate 1800
```

```
crypto pki trustpoint iosca
  enrollment url http://10.66.75.246:80 (local Giga Ethernet ip address)
  revocation-check none
  rsakeypair iosca
```

Wait 30 seconds before issuing "no shutdown" on iosca server

```
crypto pki server iosca
  no shutdown
```

```
#####
```

```
MS-3945(cs-server)#no shut
```

```
%Some server settings cannot be changed after CA certificate generation.
```

```
% Please enter a passphrase to protect the private key
```

```
% or type Return to exit
```

```
Password:Ciscotac123
```

```
Re-enter password:Ciscotac123
```

```
% Generating 1024 bit RSA keys, keys will be non-exportable...
```

```
[OK] (elapsed time was 3 seconds)
```

Jan 7 06:30:15.825: %SSH-5-ENABLED: SSH 1.99 has been enabled% Exporting Certificate Server signing certificate and keys...

% Certificate Server enabled.

Jan 7 06:30:25.384: %PKI-6-CS_ENABLED: Certificate server now enabled.

MS-3945(cs-server)#

#####

ステップ 3.設定 Trustpoints (SIP およびセキュア トランスコーダのために)

注: CUBE で登録されているセキュア トランスコーダがインターネットワーク SRTP および RTP に必要となります。

注: 統合サービス ルータ (ISR) のだけ Agregation サービス ルータ (ASR) プラットフォームにセキュア トランスコーダが、G1,G2 必要となりません。

```
crypto pki trustpoint cube3945
```

```
enrollment url http://10.66.75.246:80 (local Giga Ethernet 0/1)
```

```
serial-number none
```

```
fqdn none
```

```
subject-name CN=MS-3945.eim.com (needs to match the X.509 subject name in CUCM's secure SIP trunk profile)
```

```
ip-address none
```

```
revocation-check none
```

```
crypto pki authenticate cube3945
```

#####

```
MS-3945(config)#crypto pki authenticate cube3945
```

Certificate has the following attributes:

```
Fingerprint MD5: 2F2D61A4 EACCC730 141B2966 7370A9AA
```

```
Fingerprint SHA1: E6B86D4F C84B5453 8F63F019 773E1E0C 0DE5B883
```

```
% Do you accept this certificate? [yes/no]: yes
```

```
Trustpoint CA certificate accepted.
```

```
MS-3945(config)#
```

#####

```
crypto pki enroll cube3945
```

#####

```
MS-3945(config)#crypto pki enr cube3945
```

```
%
```

```
% Start certificate enrollment ..
```

```
% Create a challenge password. You will need to verbally provide this password to the CA Administrator in order to revoke your certificate.
```

```
For security reasons your password will not be saved in the configuration.
```

```
Please make a note of it.
```

```
Password:Ciscotac123
```

```
Jan 7 06:31:06.884: %CRYPTO-6-AUTOGEN: Generated new 512 bit key pair
```

```
Re-enter password:Ciscotac123
```

```
% The fully-qualified domain name will not be included in the certificate
```

```
Request certificate from CA? [yes/no]: yes
```

```
% Certificate request sent to Certificate Authority
```

```
% The 'show crypto pki certificate verbose cube3945' command will show the fingerprint.
```

```
Jan 7 06:31:24.088: CRYPTO_PKI: Certificate Request Fingerprint MD5: 9A128490 01A60E1D 9F3C3253 48706E5F
```

```
Jan 7 06:31:24.088: CRYPTO_PKI: Certificate Request Fingerprint SHA1: 733EE8B1 DBB0F25C 595D48E3 0830047C 50DEFB16
```

```
MS-3945(config)#
Jan  7 06:31:29.156: %PKI-6-CERTRET: Certificate received from Certificate Authority
#####
```

```
crypto pki trustpoint secdsp
  enrollment url http://10.66.75.246:80
  serial-number
  revocation-check none
  rsakeypair iosca

crypto pki authenticate secdsp (same procedure as other trustpoints)
crypto pki enroll secdsp (same procedure as other trustpoints)
```

```
sccp local GigabitEthernet0/1
sccp ccm 10.66.75.246 identifier 10 version 7.0
sccp
!

!
sccp ccm group 20
  associate ccm 10 priority 1
  associate profile 20 register XCODER_IOS

!
dspfarm profile 20 transcode universal security
  trustpoint secdsp
  codec g711ulaw
  codec g711alaw
  codec g729ar8
  codec g729abr8
  maximum sessions 10
  associate application SCCP
!
telephony-service
  secure-signaling trustpoint secdsp
  tftp-server-credentials trustpoint scme
  sdspfarm units 10
  sdspfarm transcode sessions 128
  sdspfarm tag 1 XCODER_IOS
  max-ephones 50
  max-dn 300
  ip source-address 10.66.75.246 port 2000
```

The Secure transcoder must be showing up and action by following command,

```
MS-3945#sh sccp
SCCP Admin State: UP
Gateway Local Interface: GigabitEthernet0/1
  IPv4 Address: 10.66.75.246
  Port Number: 2000
IP Precedence: 5
User Masked Codec list: None
Call Manager: 10.66.75.246, Port Number: 2000
  Priority: N/A, Version: 7.0, Identifier: 10
  Trustpoint: N/A
```

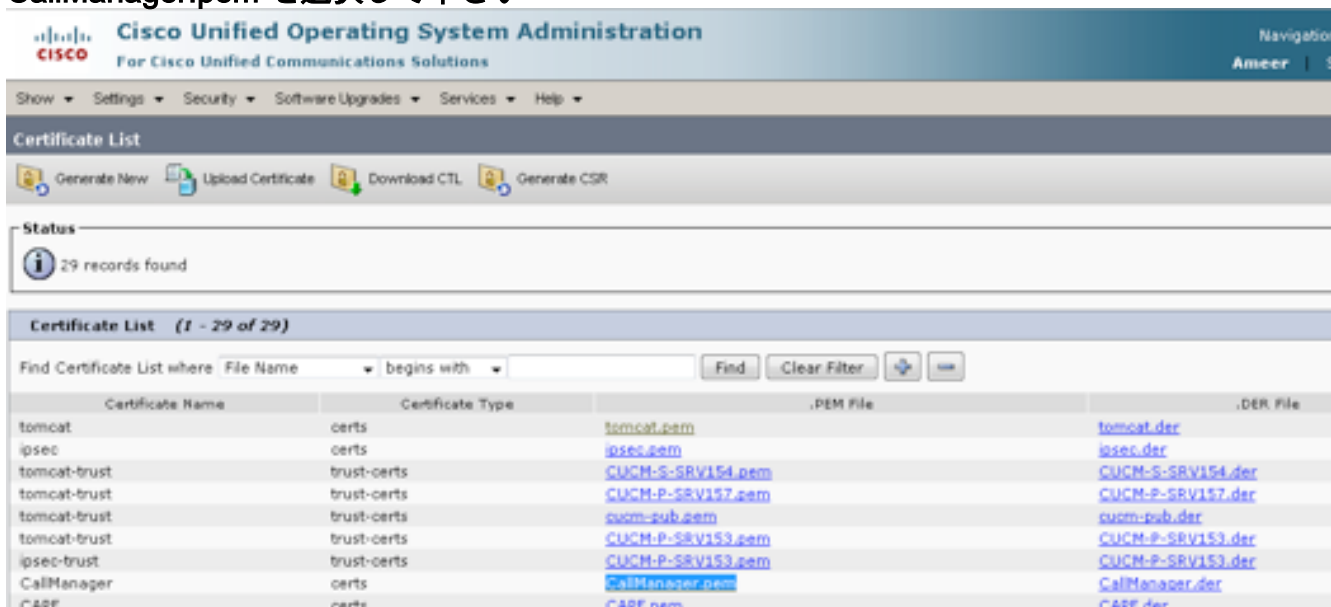
```
Transcoding Oper State: ACTIVE - Cause Code: NONE
Active Call Manager: 10.66.75.246, Port Number: 2443
TCP Link Status: CONNECTED, Profile Identifier: 20
Security
  Signaling Security: ENCRYPTED TLS
```

Media Security: SRTP
 Supported crypto suites :AES_CM_128_HMAC_SHA1_32
 Reported Max Streams: 20, Reported Max OOS Streams: 0
 Supported Codec: g711ulaw, Maximum Packetization Period: 30
 Supported Codec: g711alaw, Maximum Packetization Period: 30
 Supported Codec: g729ar8, Maximum Packetization Period: 60
 Supported Codec: g729abr8, Maximum Packetization Period: 60
 Supported Codec: rfc2833 dtmf, Maximum Packetization Period: 30
 Supported Codec: rfc2833 pass-thru, Maximum Packetization Period: 30
 Supported Codec: inband-dtmf to rfc2833 conversion, Maximum Packetization Period: 30
 TLS : ENABLED

ステップ 4. CUCM のための信頼ポイントを設定し、CUBE の CUCM 認証を登録して下さい。

```
MS-3945(config)#crypto pki trustpoint cucm50
MS-3945(ca-trustpoint)# enrollment terminal
MS-3945(ca-trustpoint)# revocation-check none
```

- CUCM (オペレーティングシステム) OS 管理 ページのこの場合ログイン:
- セキュリティ > Certificate Management > 検索
- CallManager.pem を選択して下さい



- 認証を『Download』を選択し、ように .pem ファイル保存して下さい
- テキストエディタの .pem ファイルを開いて下さい
- コピーして下さいから 「-----BEGIN CERTIFICATE-----」まで 「-----END CERTIFICATE-----」
- 例として cube3945 に認証をコピーして下さい

```
crypto pki authenticate cucm50
```

After entering the command paste the certificate and press two times enter after END CERTIFICATE.

```
#####
```

```
MS-3945(config)#crypto pki authenticate cucm-pub
```

Enter the base 64 encoded CA certificate.

End with a blank line or the word "quit" on a line by itself

```
-----BEGIN CERTIFICATE-----
```

```
MIICszCCAhygAwIBAgIIFOPHF1lcCUbcwDQYJKoZIhvcNAQEFBQAwXzEWMBQGA1UE
AwNQN1VDTs1QLVNSVjE1MzEMMAoGA1UECwwDVVEFDMQ4wDAYDVQQKDAVDSVNDTzEM
MAoGA1UEBwwDQKFOmQwCgYDVQQIDANLQVIXCzAJBgNVBAYTAk1OMB4XDTEwMTEEx
```

```
NjEyMDUwMloXDTE2MTEFNjEyMDUwMlowXzEWMBQGA1UEAwNQ1VDTs1QLVNSVjE1
MzEMMAoGA1UECwwDVFEFDMQ4wDAYDVQQKDAVDSVNDTzEMMAoGA1UEBwwDQkFOMQww
CgYDVQQIDANLQVIxZCzAJBgNVBAYTAklOMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCB
iQKBgQCRt2YXfOMgQueval6tyMCwQw0fKCDw3bqq/63atNUhSqFpswk+04GhPqxh
Pesx6tMW3E22AGWoTjsrqYTRY7TA/p2u03yPcg00PMoxNk6VN88/FLW6YNd3rOK
TmABim1UEMVMYDFQoGhtzUxya7ZFe3vpqBnDlUrgy0q01zQzJwIDAQABo3gwdjAL
BgNVHQ8EBAMCarwwJwYDVR01BCAwHgYIKwYBBQUHAWEGCCSGAQUFBwMCBggrBgEF
BQCcDBTAfBgNVHREEGDAWhhRodHRwOi8vQ1VDTs1QLVNSVjE1MzAdBgNVHQ4EFgQU
ZIIiGxzZQV0phnLrsY8Bby3jM9S0wDQYJKoZIhvcNAQEFBQADgYEAQzIvbQm8EOSU
v+bm9oykvHLMrQXjvSgSyl08mC5koUurYa/a0yf0AjMwDMc8F/NARtktsDyjddmw
Oq0G1YMuMhloyPeb41/bbc+AjXI/d/xprOJSt1qwFI3CJjCvsWm3azC4wfl1ItZNo
4gaCwzzY2UoedUA/rHrWcYod6Vl6Adw=
-----END CERTIFICATE-----
```

Certificate has the following attributes:

Fingerprint MD5: 05813269 C50FD13F 20D65A7C 0C4CD73E
Fingerprint SHA1: 8BE549A5 FB3A856F A6B3CC8B 7C30F0DF C9280288

% Do you accept this certificate? [yes/no]: yes

Trustpoint CA certificate accepted.

% Certificate successfully imported

MS-3945(config)#

#####

- CCM グループで複数の CallManager がある場合、前の手順が、さもないければ、フェールオーバー発生しないのですべてのノードのためのトラストポイントを設定し、CallManager から認証をインポートして下さい。

ステップ 5. Call Manager CallManager でインストールするために IOS 認証をエクスポートして下さい

#####

MS-3945(config)#crypto pki export cube3945 pem terminal

% CA certificate:

-----BEGIN CERTIFICATE-----

```
MIIB+TCCAwwGwIBAgIBATANBgkqhkiG9w0BAQQFADAQMw4wDAYDVQQDEwVpb3Ny
YTAeFw0xMjAxMDcwNjMwMTVaFw0xNTAxMDYwNjMwMTVaMBAxDjAMBgNVBAMTBWlv
c3JhMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDDrZwLgX7LSPwS0iAgv6Zq
1AMzikR36zGH7Cai0/Mf0nZ9nmNRVskpSBhdGbjvj43/TzqcJLSricIkBnSHSVme
SXxo+gz2sGhgZBABBvjTJ86/kavOSD9/rFJjPNdrxgA5Jdc64qUC2SKUHYGTs0Xx
alTQid2y1UOnAwpJKx8LTQIDAQABo2MwYTAPBgNVHRMBAf8EBTADAQH/MA4GA1Ud
DwEB/wQEAwIBhjAfBgNVHSMEGDAwGBQf+4wpeDVM3rkjL5LoZkj4n4j+DAdBgNV
HQ4EFgQUH/uMKXglTN65Iy+S6GZI6+J+I/gwDQYJKoZIhvcNAQEFBQADgYEAChvx
2hhF/eD2/mCgmcDWrh86OU5VV+0I3Eiphto6I8s+y2UHPmshF3sJ+OhDsT6T+C7U
xi0g961TxvdJDBsu7gDERioW3LuJuOKj7MNYDIbCMAoBlxCLtHsZvcnsVGrar3Jt
dVh2dnKi/O6VEzCGrjBkn6RPPXXOB9aEeQ6ts2M=
```

-----END CERTIFICATE-----

% General Purpose Certificate:

-----BEGIN CERTIFICATE-----

```
MIIBrTCCARagAwIBAgIBAJANBgkqhkiG9w0BAQQFADAQMw4wDAYDVQQDEwVpb3Ny
YTAeFw0xMjAxMDcwNjMwMTVaFw0xNTAxMDYwNjMwMTVaMBwxGjAYBgNVBAMTETAw
OjI00jE00kJKOjvCokRGMFwwDQYJKoZIhvcNAQEFBQADSwAwSAJBALIXjJSbcgK3
6c4EnOs/FDrqKtwHXqhwncAh2N3k4LghdwAdsQFXGtHjefJWA6TBm/fLibLD4fW8
eoacG7fpJJKCAwEAANPME0wCwYDVR0PBAQDAgWgMB8GA1UdIwQYMBaAFB/7jC14
NUzeuSMvkuhMSovifiP4MB0GA1UdDgQWBBSW11Md2rFbqZf0IuicijOJ15PnPDAN
BgkqhkiG9w0BAQQFAA0BgQCZetK4TeNrtoQ3/3eaCD7sL/RNic8aRbNOn2KcCxyO
WmtH8xRs4Hm9lw4K4o93D3mgAP6JLAB6RN4LdzFm5S800YXTDYoeQ/kO9i9RrTFq
ARbdZRULb02tgrBjYHngQ5dV7C7hqw4CfjJeQI1UQWSibiyKT0mN8o5n/1B37G
GQ==
```

-----END CERTIFICATE-----

MS-3945(config)#

#####

- 認証をコピーし、テキストエディタでように cube3945g.pem ファイル保存して下さい。

注: 必要とされる一般目的認証だけ

- CallManager 信頼として IOS CA 認証をアップロードして下さい。
- CUCM OS 管理 ページへのナビゲート
- セキュリティ > Certificate Management > アップロード認証

ステップ 6. Cube3945 および CUCM をのための保護します電話 CP-8945 を設定して下さい

CUBE

#####

```
MS-3945(config)#crypto pki export cube3945 pem terminal
```

```
% CA certificate:
```

```
-----BEGIN CERTIFICATE-----
```

```
MIIB+TCCAwwKAgAwIBAgIBATANBgkqhkiG9w0BAQQFADAQMq4wDAYDVQQDEwVpb3Ny  
YTAeFw0xMjAxMDcwNjMwMTVaFw0xNTAxMDYwNjMwMTVaMBAxDjAMBGNVBMAMTBWlv  
c3JhMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDDrZwLgx7LSPwS0iAgv6Zq  
lAMzikR36zGH7Cai0/Mf0nZ9nmNRVskpSBhdGbjvj43/TzqcJLSricIkBnSHSVme  
SXxo+gz2sGhgZBABBVjtJ86/kaVOSD9/rFJjPNdrxgA5Jdc64qUC2SKUHYGTs0Xx  
alTQid2ylUOnAwpJKx8LTQIDAQABO2MwYTAPBgNVHRMBAf8EBTADAQH/MA4GA1Ud  
DwEB/wQEAwIBhjAfBgNVHSMEGDAwGBQf+4wpeDVM3rkjL5LoZkjr4n4j+DAdBgNV  
HQ4EFgQUH/uMKXglTN65Iy+S6GZI6+J+I/gwDQYJKoZIhvcNAQEBBQADgYEAcHvx  
2hhf/ed2/mCgmcDWrh86OU5VV+0I3Eipht06I8s+y2UhPMshF3sJ+OhDsT6T+C7U  
xi0g961TxvdJDBsu7gDERioW3LuJuOKj7MNYDIbCMaoBlxCLtHsZvcnsVGrar3Jt  
dVh2dnKi/O6VEzCGrjBkn6RPPXXOB9aEeQ6ts2M=
```

```
-----END CERTIFICATE-----
```

```
% General Purpose Certificate:
```

```
-----BEGIN CERTIFICATE-----
```

```
MIIBrTCCARagAwIBAgIBAJANBgkqhkiG9w0BAQQFADAQMq4wDAYDVQQDEwVpb3Ny  
YTAeFw0xMjAxMDcwNjMxMjRlFw0xNTAxMDYwNjMwMTVaMBwxGjAYBgNVBAMTEtAw  
OjI0OjE0OkJCOjVCOkRGMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBALixjJSbcgK3  
6c4EnOs/FDrqKtWxHqhwncAh2N3k4LghdwAdsQFXGtHjeFJWA6TBm/fLibLD4fW8  
eocG7fpJJKCAwEAANPME0wCwYDVR0PBAQDAgWgMB8GA1UdIwQYMBaAFB/7jCl4  
NUzeuSMvkuhmSoviFiP4MB0GA1UdDgQWBBSW11Md2rFbqZf0IuicijOJ15PnPDAN  
BgkqhkiG9w0BAQQFAAOBgQCZeTK4TeNrtoQ3/3eaCD7sL/RNlc8aRbNOn2KcCxyO  
WmtH8xRs4Hm9lw4K4o93D3mgAP6JLAB6RN4LdzFm5S8O0YXTDYoeQ/kO9i9RrTFq  
ARbdZRuULb02tgrBjYHngQ5dV7C7hqwR4CfjJeQI1UQWSibiyKT0mN8o5n/1B37G  
GQ==
```

```
-----END CERTIFICATE-----
```

```
MS-3945(config)#
```

#####


CUCM

- セキュア モードの CUCM のレジスタ CP-8945。
- CP-8945 のためのセキュア SCCP プロファイルを作成して下さい
- CP-8945 の設定の下でセキュア プロファイルを選択して下さい。

Phone Security Profile Configuration

 Save  Delete  Copy  Reset  Apply Config  Add New

- Status

 Status: Ready

- Phone Security Profile Information

Product Type: Cisco 8945

Device Protocol: SCCP

Name*

Description

Device Security Mode

TFTP Encrypted Config

- Phone Security Profile CAPF Information

Authentication Mode*

Key Size (Bits)*

Note: These fields are related to the CAPF Information settings on the Phone Configuration page.

Protocol Specific Information

Packet Capture Mode*

Packet Capture Duration

Presence Group*

Device Security Profile*

SUBSCRIBE Calling Search Space

Unattended Port

Require DTMF Reception

RFC2833 Disabled

- 保存し、CP-8945 設定をリセットして下さい、それを良く登録します確認して下さい
- CUBE の方の SIP トランクのセキュア SIP プロファイルを適用して下さい

SIP Trunk Security Profile Configuration

Save
 Delete
 Copy
 Reset
 Apply Config
 Add New

Status

Status: Ready

SIP Trunk Security Profile Information

Name*

Description

Device Security Mode

Incoming Transport Type*

Outgoing Transport Type

Enable Digest Authentication

Nonce Validity Time (mins)*

X.509 Subject Name

Incoming Port*

Enable Application level authorization

Accept presence subscription

Accept out-of-dialog refer**

Accept unsolicited notification

Accept replaces header

Transmit security status

Allow charging header

SIP V.150 Outbound SDP Offer Filtering*

• SIP トランク の 設定

Media Termination Point Required
 Retry Video Call as Audio
 Path Replacement Support
 Transmit UTF-8 for Calling Party Name
 Transmit UTF-8 Names in QSIG APDU
 Unattended Port
 SRTP Allowed - When this flag is checked, Encrypted TLS needs to be configured in the network to provide end to end security. Failure to do so will expose keys and other information.
 Consider Traffic on This Trunk Secure*
 Route Class Signaling Enabled*
 Use Trusted Relay Point*
 PSTN Access
 Run On All Active Unified CM Nodes

-SIP Information-

Destination

Destination Address is an SRV

Destination Address	Destination Address IPv6	Destination Port
1* 10.66.75.246		5061

MTP Preferred Originating Codec* G729/G729a

Presence Group* Standard Presence group

SIP Trunk Security Profile* Secure SIP Trunk Profile

Rerouting Calling Search Space <None >

Out-Of-Dialog Refer Calling Search Space <None >

SUBSCRIBE Calling Search Space <None >

SIP Profile* TEST_SIP_Profile

DTMF Signaling Method* No Preference

- テスト コールを使うと、コールが SRTP に CUBE の RTP にあり、CP-8945 画面のロックアイコンが確認することを確認するために表示コマンドを使用できません、電話と CUBE 間に SRTP があります

MS-3945#sh sccp conn

sess_id	conn_id	stype	mode	codec	sport	rport	ripaddr	conn_id_tx
458757	20	s-xcode	sendrecv	g711u	16770	2000	10.66.75.246	
458757	24	xcode	sendrecv	g711u	16768	2000	10.66.75.246	

Total number of active session(s) 1, and connection(s) 2

MS-3945#sh call active voice brief

```
<ID>: <CallID> <start>ms.<index> (<start>) +<connect> pid:<peer_id> <dir> <addr> <state>
dur hh:mm:ss tx:<packets>/<bytes> rx:<packets>/<bytes> dscp:<packets violation> media:<packets
violation> audio tos:<audio tos value> video tos:<video tos value>
IP <ip>:<udp> rtt:<time>ms pl:<play>/<gap>ms lost:<lost>/<early>/<late>
delay:<last>/<min>/<max>ms <codec> <textrelay> <transcoded>

media inactive detected:<y/n> media cntrl rcvd:<y/n> timestamp:<time>

long duration call detected:<y/n> long duration call duration :<sec> timestamp:<time>
MODEMPASS <method> buf:<fills>/<drains> loss <overall%> <multipkt>/<corrected>
last <buf event time>s dur:<Min>/<Max>s
FR <protocol> [int dlci cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
<codec> (payload size)
ATM <protocol> [int vpi/vci cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
<codec> (payload size)
Tele <int> (callID) [channel_id] tx:<tot>/<v>/<fax>ms <codec> noise:<l> acom:<l> i/o:<l>/<l>
dBm
MODEMRELAY info:<rcvd>/<sent>/<resent> xid:<rcvd>/<sent> total:<rcvd>/<sent>/<drops>
speeds(bps): local <rx>/<tx> remote <rx>/<tx>
Proxy <ip>:<audio udp>,<video udp>,<tcp0>,<tcp1>,<tcp2>,<tcp3> endpt: <type>/<manf>
bw: <req>/<act> codec: <audio>/<video>
tx: <audio pkts>/<audio bytes>,<video pkts>/<video bytes>,<t120 pkts>/<t120 bytes>
rx: <audio pkts>/<audio bytes>,<video pkts>/<video bytes>,<t120 pkts>/<t120 bytes>
```

Telephony call-legs: 0

SIP call-legs: 2

H323 call-legs: 0

Call agent controlled call-legs: 0

SCCP call-legs: 2

Multicast call-legs: 0

Total call-legs: 4

0 : 32138 423566780ms.1 (02:08:15.881 UTC Tue Feb 5 2013) +2270 pid:2088 Answer 1005 active
dur 00:00:35 tx:1761/281760 rx:1753/280480 dscp:0 media:0 audio tos:0xB8 video tos:0x0
IP 10.66.75.178:24714 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay:
off Transcoded: Yes
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a

0 : 32139 423566790ms.1 (02:08:15.891 UTC Tue Feb 5 2013) +2250 pid:1006 Originate 2088
active
dur 00:00:35 tx:1753/287492 rx:1761/288804 dscp:0 media:0 audio tos:0xB8 video tos:0x0
IP 10.66.75.76:22512 SRTP: on rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off
Transcoded: Yes
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a

0 : 32142 423569050ms.1 (02:08:18.151 UTC Tue Feb 5 2013) +0 pid:0 Originate connecting
dur 00:00:35 tx:1761/281760 rx:1753/280480 dscp:0 media:0 audio tos:0x0 video tos:0x0
IP 10.66.75.246:2000 SRTP: off rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay:
off Transcoded: No
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a

0 : 32144 423569050ms.2 (02:08:18.151 UTC Tue Feb 5 2013) +0 pid:0 Originate connecting
dur 00:00:35 tx:1753/287492 rx:1761/288804 dscp:0 media:0 audio tos:0x0 video tos:0x0
IP 10.66.75.246:2000 SRTP: on rtt:0ms pl:0/0ms lost:0/0/0 delay:0/0/0ms g711ulaw TextRelay: off
Transcoded: No
media inactive detected:n media contrl rcvd:n/a timestamp:n/a
long duration call detected:n long duration call duration:n/a timestamp:n/a

Telephony call-legs: 0
SIP call-legs: 2
H323 call-legs: 0
Call agent controlled call-legs: 0
SCCP call-legs: 2
Multicast call-legs: 0
Total call-legs: 4

関連情報

- [CUCM セキュリティ ガイド](#)
- [CUBE コンフィギュレーション ガイド](#)